IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (previously presented) A method fairly exchanging a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values, comprising the steps of:

establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values wherein each said sequence value is related, according to said modular function, to a next previous sequence value, whereby conformance to the modulation function can be determined for adjacent ones of the plurality of sequence values;

establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user;

iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values;

completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed.

2. (canceled)

3. (previously presented) The method of claim 1, wherein said plurality of values are determined according to the modular function by a root value and a modulus value.

4. (previously presented) The method of claim 1, wherein said sequence values are determined over a known order equal to the total number of iterations, wherein each said sequence value is a result of the modular function applied to a next previous sequence

value, raised to a power related to a difference in position between said sequence value and a respective beginning and end of the order.

5. (canceled)

6. (previously presented) The method of claim 4, wherein said modulus value is a product of Blum integers.

7. (previously presented) The method of claim 6, wherein said Blum integers comprise prime numbers.

8. (canceled)

9. (previously presented) The method of claim 1, wherein said hidden value is a value immediately preceding a last value of said sequence.

10. (previously presented) The method of claim 1, wherein said number of iterations is at least 80.

11 - 22. (canceled)

23. (previously presented) A system for exchanging user information over a network comprising:

at least one programmed processor coupled to a memory and arranged for conducting a fair exchange of a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values;

establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values wherein each said sequence value is related, according to said modular function, to

a next previous sequence value, whereby conformance to the modular function can be determined for adjacent ones of the plurality of sequence values;

establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user,

iteratively exchanging the sequence values of the first and second users, progressing toward an end of said sequence values;

completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed.

24. (previously presented) The system of claim 23, further comprising a further processor and wherein said processor and said further processor exchange said sequence values on behalf of the first and second users, respectively.

25. (previously presented) The system of claim 23, wherein said processor is operable to effect the series of exchanges on a timed-basis.

26 - 29. (canceled)